Monotone circuit lower bounds

Lukáš Folwarczný

folwarczny@math.cas.cz

Institute of Mathematics of the Czech Academy of Sciences

Computer Science Institute of Charles University in Prague

November 11, 2020

Monotone Boolean functions

- For $x, y \in \{0,1\}^n$ we write $x \leq y$ iff $(\forall i \in \{1,\ldots,n\}) x_i \leq y_i$.
- A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is monotone iff $x \leq y$ implies $f(x) \leq f(y)$.
- Monotone Boolean functions may be represented by DNFs or CNFs without negations.
- Examples:
    - Threshold functions $\mathrm{Th}_k^n(x) = 1$ iff $x_1 + \cdots + x_n \geq k$.
    - $\mathrm{CLIQUE}(n,k)\colon \{0,1\}^{\binom{n}{2}} \to \{0,1\}$
        - Input x encodes graph G_x with vertices $\{1,\ldots,n\}$, where i and j are adjacent iff $x_{ij} = 1$.
        - $\mathrm{CLIQUE}(n,k)(x) = 1$ iff G_x contains a clique on k vertices.

Monotone Boolean circuits

- Circuits with fanin-2 AND and OR gates.
  - Small technical detail: We should allow constants 0 and 1 to be able to compute all monotone Boolean functions including the constant ones.
- For a circuit C, size(C) is the number of gates.

Lower bounds

Lower bounds for explicit functions of n variables.

- Tiekenheinrich [Tie84]: $4n$
- Razborov [Raz85]: $n^{\Omega(\log n)}$
- Andreev [And85]: $2^{n^{c-o(1)}}$ [1] independently of Razborov
- Andreev [And87]: $2^{\Omega(n^{1/3}/\log n)}$
- Harnik and Raz [HR00]: $2^{\Omega((n/\log n)^{1/3})}$
- Cavalar, Kumar and Rossman [preprint 2020]: $2^{\Omega(n^{1/2}/(\log n)^{3/2})}$

[1] I was not able to find the value of c.

Theorem ([Raz85], [AB87])

For $3 \leq k \leq n^{1/4}$, the monotone circuit complexity of $\mathrm{CLIQUE}(n,k)$ *is* $n^{\Omega(\sqrt{k})}$.

I follow the proof from the book by Jukna [Juk12].

Combinatorial tool: The sunflower lemma

Definition

A *sunflower with p petals and a core T* is a collection of sets $S_1, \ldots, S_p$ such that $S_i \cap S_j = T$ for all $i \neq j$.

Theorem (Sunflower lemma [ER60])

Let $\mathcal{F}$ be a family of sets each of size at most l. If $|\mathcal{F}| > l!(p-1)^l$ then $\mathcal{F}$ contains a sunflower with p petals.

Proof by induction on l:

- $l = 1$: We have more than $p-1$ sets of cardinality ≤ 1, any p of them form a sunflower with empty core.
- $l \geq 2$:
  - $\mathcal{S} = \{S_1, \ldots, S_t\}$ a maximal family of pairwise disjoint members of $\mathcal{F}$
  - If $t \geq p$: We are done.
  - Assume $t \leq p-1$. $S := S_1 \cup \cdots \cup S_t$. $|S| \leq l(p-1)$.
  - S intersects (by maximality) every set in $\mathcal{F}$
  - Pigeonhole principle: exists $x \in S$ lying in at least this many sets of $\mathcal{F}$:

$$\frac{|\mathcal{F}|}{|S|} > \frac{l!(p-1)^l}{l(p-1)} = (l-1)!(p-1)^{l-1}$$

  - $$\mathcal{F}_x := \{F \setminus \{x\} \mid F \in \mathcal{F}, x \in F\}$$
  - Apply the induction assumption on $\mathcal{F}_x$ and add x to each petal.

Razborov's Method of Approximations

- The set of all monotone Boolean functions $\to$ the set of approximators $\mathcal{A}$
  - Input variables are in the set of approximators
- New operations: $\vee \to \sqcup$, $\wedge \to \sqcap$
  - $\sqcup, \sqcap$: $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$
- Circuit C computing $\mathrm{CLIQUE}(n, k) \to$ approximator circuit $\tilde{C} \in \mathcal{A}$
- Strategy of the proof:
  - Every approximator (including $\tilde{C}$) makes a lot of errors when computing $\mathrm{CLIQUE}(n, k)$.
  - If $\mathrm{size}(C)$ is small, then $\tilde{C}$ cannot make too many errors.
  - This together implies that $\mathrm{size}(C)$ is large.

Our approximators

- For $X \subseteq \{1, \ldots, n\}$, the *clique indicator* of X is the function $\lceil X \rceil$:

$$\lceil X \rceil(E) = 1 \text{ iff the graph } E \text{ contains a clique on the vertices } X$$

- $\lceil X \rceil$ is just a monomial

$$\lceil X \rceil = \bigwedge_{i,j \in X; i<j} x_{ij}$$

- (m, l)-*approximator* is an OR of at most m clique indicators. The underlying vertex-set X of each indicator satisfies $|X| \leq l$.
- $m, l \geq 2$ to be set later
- Observe that input variables x_{ij} are (m, l)-approximators because

$$x_{ij} = \lceil \{i, j\} \rceil.$$

Positive and negative graphs

- *Positive graphs*: $\mathcal{P}$ denotes the set of all graphs on n vertices which consist of one clique on k vertices and $n-k$ isolated vertices.
  - $|\mathcal{P}| = \binom{n}{k}$
  - $(\forall E \in \mathcal{P}) C(E) = 1$
- *Negative graphs*: $\mathcal{N}$ denotes the **multiset** of all the graphs on n vertices created by the following process: We color each vertex by one of $k-1$ colors and then connect by edges pairs of vertices with different colors.
  - $|\mathcal{N}| = (k-1)^n$
  - $(\forall E \in \mathcal{N}) C(E) = 0$

Each approximator makes a lot of errors

Lemma

Every approximator either rejects all graphs or wrongly accepts at least a fraction $1 - l^2/(k-1)$ *of all* $(k-1)^n$ *negative graphs.*

- An (m, l)-approximator $A = \bigvee_{i=1}^{r} \lceil X_i \rceil$.
- Assume that A accepts at least one graph. Then $A \geq \lceil X_1 \rceil$.
- A negative graph is rejected by $\lceil X_1 \rceil$ iff its associated coloring assigns some two vertices of X_1 the same color.
- There are $\binom{|X_1|}{2}$ pairs of vertices in X_1. For each such pair at most $(k-1)^{n-1}$ colorings assign the same color.
- Thus, at most $\binom{|X_1|}{2}(k-1)^{n-1} \leq \binom{l}{2}(k-1)^{n-1}$ negative graphs can be rejected by $\lceil X_1 \rceil$, and hence, by the approximator A.

Operation $\sqcup$

- Two (m,l)-approximators $A = \bigvee_{i=1}^{r} \lceil X_i \rceil$ and $B = \bigvee_{i=1}^{s} \lceil Y_i \rceil$ are given.
- We wish to define an (m,l)-approximator $A \sqcup B$ that approximates $A \vee B$
- Defining $A \sqcup B = A \vee B$ would potentially give us $(2m,l)$-approximator. We use the sunflower lemma to overcome this:
  - $\mathcal{F} := \{X_1, \ldots, X_r, Y_1, \ldots, Y_s\}$
  - $m := l!(p-1)^l$
  - Plucking: replace the p sets forming a sunflower by their core
  - Plucking procedure: repeat plucking while $r + s > m$
  - Each plucking reduces the number of sets $\Rightarrow$ at most m pluckings

Operation $\sqcap$

- Two (m,l)-approximators $A = \bigvee_{i=1}^{r} \lceil X_i \rceil$ and $B = \bigvee_{i=1}^{s} \lceil Y_i \rceil$ are given.
- We wish to define an (m,l)-approximator $A \sqcap B$ that approximates $A \wedge B$
- Defining

$$A \sqcup B = A \wedge B = \bigvee_{i=1}^{r} \bigvee_{j=1}^{s} (\lceil X_i \rceil \wedge \lceil Y_j \rceil)$$

  has two issues:
  - up to m^2 terms
  - $\lceil X_i \rceil \wedge \lceil Y_j \rceil$ might not be a clique indicator
- We do the following steps:
  1. Replace the term $\lceil X_i \rceil \wedge \lceil Y_j \rceil$ by the clique indicator $\lceil X_i \cup Y_j \rceil$.
  2. Erase those indicators $\lceil X_i \cup Y_j \rceil$ with $|X_i \cup Y_j| \geq l+1$.
  3. Apply the plucking the procedure to the remaining indicators; there will be at most m^2 pluckings.

Lemma (Error on positive graphs)

$$|\{E \in \mathcal{P} | \tilde{C}(E) = 0\}| \leq \text{size}(C) \cdot m^2 \binom{n-l-1}{k-l-1}$$

- We calculate the number of errors introduced by a single gate.
- Case 1: $\vee$-gate is replaced by $\sqcup$
  - This involves taking $A \vee B$ and the plucking procedure.
  - Each plucking replaces a clique indicator $\lceil X \rceil$ with some indicator $\lceil X' \rceil$ s.t. $X' \subseteq X$ which can only accept more graphs, i.e., no error is introduced.

- Case 2: $\wedge$-gate is replaced by $\sqcap$
  - The first step was to replace $\lceil X_i \rceil \wedge \lceil Y_j \rceil$ by $\lceil X_i \cup Y_j \rceil$. These functions behave identically on positive graphs (cliques).
  - The second step was to erase those clique indicators $\lceil X_i \cup Y_j \rceil$ for which $|X_i \cup Y_j| \geq l+1$. For each such clique indicator, at most $\binom{n-l-1}{k-l-1}$ of the positive graphs are lost. There are at most m^2 of these indicators.
  - The third step was the plucking procedure which again accepts only more graphs.
- In total, the error is at most $\text{size}(C) \cdot m^2 \binom{n-l-1}{k-l-1}$.

Lemma (Error on negative graphs)

$$|\{E \in \mathcal{N} | \tilde{C}(E) = 1\}| \leq \text{size}(C) \cdot m^2 l^{2p} (k-1)^{n-p}$$

- We again calculate the number of errors introduced by a single gate.
- We analyze the number of errors introduced by plucking:
  - Sunflower with core Z and petals $Z_1, \ldots, Z_p$.
  - Let $\mathbf{G}$ be a uniformly random graph from $\mathcal{N}$ – this correponds to coloring each vertex independently by one of the $k-1$ colors, each color having probability $1/(k-1)$.
  - What is the probability that $\lceil Z \rceil$ accepts $\mathbf{G}$, but none of the $\lceil Z_1 \rceil, \ldots, \lceil Z_p \rceil$ accept it?
  - PC stands for "properly colored"

$$
\begin{aligned}
&\Pr[Z \text{ is PC and } Z_1, \ldots, Z_p \text{ are not PC}] \\
&\quad \leq \Pr[Z_1, \ldots, Z_p \text{ are not PC} | Z \text{ is PC}] \\
&\quad = \prod_{i=1}^{p} \Pr[Z_i \text{ is not PC} | Z \text{ is PC}] \\
&\quad \leq \prod_{i=1}^{p} \Pr[Z_i \text{ is not PC}] \\
&\quad \leq (\binom{l}{2}/(k-1))^p \leq l^{2p}(k-1)^{-p}
\end{aligned}
$$

- The lines hold because:
    1. The definition of conditional probability
    2. Sets $Z_i \setminus Z$ are disjoint and hence the events are independent.
    3. It is less likely to happen that Z_i is not PC given the fact that Z is PC.
    4. Z_i is not PC iff two vertices get the same color

- Thus, one plucking adds at most $l^{2p}(k-1)^{n-p}$ negative graphs which are accepted.
- Case 1: $\vee$-gate is replaced by $\sqcup$
  - We take $A \vee B$ and perform at most m pluckings.
- Case 2: $\wedge$-gate is replaced by $\sqcap$
  - The first step introduces no error because $\lceil X_i \rceil \wedge \lceil Y_j \rceil \geq \lceil X_i \cup Y_j \rceil$.
  - The second step introduces no error because we only remove indicators, which cannot accept more graphs.
  - The third step involves at most m^2 pluckings.
- In both cases: at most $m^2 l^{2p}(k-1)^{n-p}$ negative graphs are newly accepted.

Grand finale

- Set $l = \lfloor \sqrt{k-1}/2 \rfloor$; $p = \lfloor 10\sqrt{k} \log_2 n \rfloor$
- Recall $m = l!(p-1)^l \leq (pl)^l$. See $m^2 \leq (10k \log_2 n)^{\sqrt{k}}$
- Use the first lemma
- Case 1: $\tilde{C}$ is identically 0
    - $\tilde{C}$ errs on all positive graphs, we obtain:

$$\text{size}(C) \cdot m^2 \cdot \binom{n-l-1}{k-l-1} \geq \binom{n}{k}$$

$$\text{size}(C) \geq \frac{(n/k)^{l+1}}{m^2} \geq \frac{n^{3/4 \cdot (\lfloor \sqrt{k-1}/2 \rfloor + 1)}}{(10 n^{1/4} \log_2 n)^{\sqrt{k}}} = n^{\Omega(\sqrt{k})}$$

- Case 2: $\tilde{C}$ outputs 1 on a $(1 - l^2/(k-1)) \geq 1/2$ fraction of all $(k-1)^n$ graphs

$$\text{size}(C) \cdot m^2 \cdot 2^{-p} \cdot (k-1)^n \geq \frac{1}{2}(k-1)^n$$

$$\text{size}(C) \geq \frac{2^p}{2m^2} = \frac{n^{9\sqrt{k}}}{2(10k \log_2 n)^{\sqrt{k}}} \geq n^{\Omega(\sqrt{k})}$$

References

[AB87] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Comb.*, 7(1):1–22, 1987.

[And85] A. E. Andreev. On a method for obtaining lower bounds for the complexity of individual monotone functions. *Soviet Math. Dokl.*, 31(3):530–534, 1985.

[And87] A. E. Andreev. A method for obtaining efficient lower bounds for monotone complexity. *Algebra and Logic*, 26:1–18, 1987.

[ER60] P. Erdös and R. Rado. Intersection theorems for systems of sets. *Journal of the London Mathematical Society*, s1-35(1):85–90, 1960.

[HR00] Danny Harnik and Ran Raz. Higher lower bounds on monotone size. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 378–387. ACM, 2000.

[Juk12] Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*, volume 27 of *Algorithms and combinatorics*. Springer, 2012.

[Raz85] A. A. Razborov. Lower bounds for the monotone complexity of some boolean functions. *Soviet Math. Dokl.*, 31:354–357, 1985.

[Tie84] Jürgen Tiekenheinrich. A 4n-lower bound on the monotone network complexity of a one-output boolean function. *Inf. Process. Lett.*, 18(4):201–202, 1984.